Version 1.1 October 2020

China CITIC Bank

London Branch

BUSINESS CONTINUITY PLAN

2020

中信银行 CHINA CITIC BANK 伦敦分行 LONDON BRANCH

Document Control

Owner	Chief Risk Officer	**Status**	FINAL
Version	1.1	**Approved by**	ARCo
Approval Date	26/11/2020	**Next Review Date**	September 2021

Version Control

Version	Author	Approval	Date	Key Changes
1.0	G Lowe	ARCO		Initial document including WFH VPN capability

Contents

1. Introduction

China CITIC Bank, London Branch ("CNCBLB or the Branch") is fully supported by Head Office at the highest level of management with senior management and departmental oversight, outsourced IT systems and liquidity facilities.

The 2018 Regulatory Business plans lays out the Business Continuity Plan ("BCP") high-level concept with the Branch operating within the HO "Two Cities Three Centres" disaster recovery ("DR") infrastructure, whereby two data centres are operated in Beijing, and another back-up is kept in the city of Xi'an (***see Appendix 1***). This facilitates all aspects of the Branch BCP, both IT and non-IT related incidents are able to be successfully carried out. This includes the following:

- Over 200 staff focused on all areas of DR including site, networks, core systems, applications and platforms;
- In case of a failure of the Beijing production IT environment, HO Data Centre staff will conduct a disaster recovery switchover, if required, to resume the affected systems (including overseas systems);
- HO Data Centre keeps system contingency plans and provides continuous system monitoring and maintenance. Urgent production issues are dealt with at the point of occurrence;
- For key business systems, the agreed recovery time objective ("RTO") is 2 hours and recovery point objective ("RPO") is 0 (this is defined in a SLA between HO and London Branch);
- London Branch has full VPN capabilities to access all three IT environments, this includes the internet, intranet and business production environments.
- London Branch can reconnect to the system to resume business processing, after the HO system switchover; and
- To familiarise the process and validate the DR operations, London Branch will participate in joint DR testing with HO at least once per annum.

This document provides more granular detail on CNCBLB's strategy, plans and management actions to ensure independent business continuity. Even though CNCBLB has no production systems physically installed in London (***see Appendix 2***), CNCBLB has deploy network infrastructure and some local supportive IT systems (e.g. virtual desktops and event monitors) to support the local daily business operations.

To ensure continuous business service, CNCBLB has the necessary disaster recovery arrangements in place, including a backup server room, standby networking, server and storage devices. Important data of the Branch (primarily shared documents within the branch) is copied from the production server room to the backup server room.

If the London production server room fails, the IT network and services will be restored in the backup server room and normal business services will resume. In case of damage to the office severe, Branch IT staff could go to DR site for the manual DR fail-over of the following:

- Storage and Network Attached Storage ("NAS") (failover);
- Virtual machines and virtual desktops (import and restart); and
- Trade PCs (power on).

The planned RTO is set to be less than 2 hours, with the planned RPO approximately 2 hours using local data.

2. Objectives

The primary objectives of this BCP are:-

- To mitigate against the risk of an incident occurring;
- To protect employees and visitors and minimise the risk of personal injury;
- To maintain acceptable levels of business and service, meeting ongoing obligations to clients, regulators, parent, and other stakeholders, within defined, agreed timescales, given the circumstances prevailing at that time;
- To establish an effective 'Incident management' and communications structure that will operate in the event of an incident;
- To test and validate solutions and procedures on a regular basis; and
- To embed business continuity principles into business as usual work practices allowing the business continuity solution to develop as products, services, responsibilities or processes change

It is the responsibility of all staff and Heads of Departments to assist Risk department in identifying, managing and monitoring the inherent and emerging operational resilience risk factors to ensure CNCBLB can continue its business operations.

3. Policy Ownership/Oversight

The 'chain' of ownership and oversight of this policy is set out below:

Document Owner	The Branch's Chief Risk Officer ("CRO") is responsible for the maintenance for this policy. The CRO will also be responsible for reviewing the ongoing adequacy of the policy and will review it on an annual basis. Any material changes to this policy must be formally signed off by the Management Committee ("ManCo") before these changes are communicated to staff.
Challenge	The Audit and Risk Committee ("ARCo") will review and challenge this policy at least annually or more frequently as necessary. A recommendation for approval or otherwise must be made to the ManCo following each review. Reviews outside the annual cycle could be prompted by changes made to the President's delegation of authority ("DOA") from HO; or changing regulatory requirements.
Approval	ARCo reviews, challenges and approves the policy based on the recommendation of RMD and CRO. ManCo will have oversight of ARCo policies and if satisfied, will ratify the approved policy.
Applicability	All members of staff, whether permanent (local hires and/or expatriate) or contractors must operate in accordance with this policy. Escalation of any matters arising in respect of this should be via the individual's Head of Department or directly to the CRO. To ensure compliance with the requirements of this policy the Risk Department and well as Internal Audit will conduct periodic reviews to ascertain compliance with the provisions of this policy.

4. UK Regulatory requirements

CNCBLB is regulated by both the PRA and FCA (known collectively as the UK bank Regulators"), and Business Continuity guidance is mainly given under the 'Systems & Control' rules and guidelines. The BCP is covered and managed under the Operational Risk Management framework and considers both:

SYSC 3.2.19 - A *firm* should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness.

SYSC 13.8 - A *firm* should consider the likelihood and impact of a disruption to the continuity of its operations from unexpected events. This should include assessing the disruptions to which it is particularly susceptible (and the likely timescale of those disruptions) including through:

- loss or failure of internal and external resources (such as people, systems and other assets);
- the loss or corruption of its information; and
- external events (such as vandalism, war and "acts of God").

A *firm* should document its strategy for maintaining continuity of its operations, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy.
A *firm* should establish:

- formal business continuity plans that outline arrangements to reduce the impact of a short, medium or long-term disruption, including:
    - resource requirements such as people, systems and other assets, and arrangements for obtaining these resources;
    - the recovery priorities for the *firm's* operations; and
    - communication arrangements for internal and external concerned parties (including the *FCA*, *clients* and the press)
- escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;
- processes to validate the integrity of information affected by the disruption; and

- processes to review and update (1) to (3) following changes to the *firm's* operations or risk profile (including changes identified through testing).

The use of an alternative site for recovery of operations is common practice in business continuity management. A *firm* that uses an alternative site should assess the appropriateness of the site, particularly for location, speed of recovery and adequacy of resources. Where a site is shared, a *firm* should evaluate the risk of multiple calls on shared resources and adjust its plans accordingly.

The Bank of England and FCA provided a consultation paper on 'Operational Resilience' which covers a broad range of risks that Firms should be monitoring and have a risk oversight, this includes but is not limited to:

- Human Resources Management;
- Crisis Management & Communication;
- Incitement response & business continuity;
- ICT and information security;
- Supply chain management; and
- Organisational behaviour

5. Incident Management

In the event of an incident, the Bank's main priority will always be the safety and welfare of its staff and the Heads of Department are responsible for cascading to their teams, the contents of this plan and making them aware of what they should do in the event of an incident. To reduce unnecessary delays in recovering the business in the event of an incident, this plan must be fully understood by all affected staff members and tested regularly.

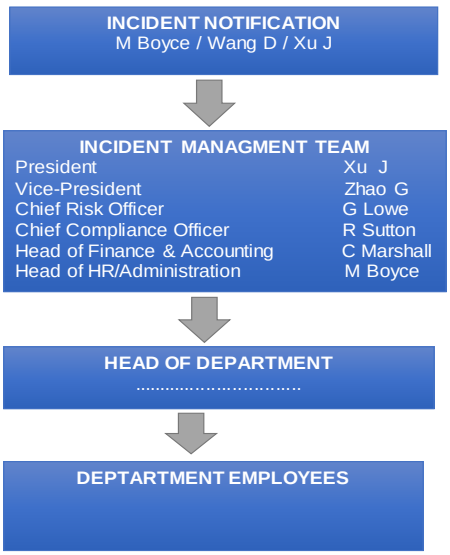
The objective of this plan is to re-establish business operations as quickly as possible and to a level that:

- Customer relations are maintained
- Regulatory requirements are met
- Reputation is upheld
- Losses are controlled and kept to a minimum
- The immediate and medium term survival of the business is assured

This plan covers the departments located in 5F, 99 Gresham Street, London (EC2V 7NG) and details the key activities, which were identified through the Business Impact Analysis exercise (see Section 8), and how these key activities will be recovered in the event of an incident.

The Incident Management Team (IMT) is made up of the Management Committee members and Head of Human Resources. Should an incident occur we expected the following communication cascade:

COMMUNICATION CASCADE



The IMT will:-

- Assess the impact of the incident and determine what actions to take to support the business, including the scaling back of business operations or invoking the use of the disaster recovery site;
- Manage the progress of the incident and the implementation of the Bank's response to the situation delegating specific responsibilities as appropriate ;
- Determine an appropriate recovery strategy, including considering any salvage requirements and options;
- Manage internal and external communication with the local authorities and emergency services including liaison with, Head Office, Clients, Counterparties, regulators, other key stakeholders and the media;
- Address staff welfare concerns including managing contact with next of kin;
- Maintain a log of key decisions and actions taken;
- Perform a post-event review to review the actions taken and to assess the outcome of the situation;
- To authorise the necessary resources and expenditure to achieve business recovery.

The Heads of Department will have their own departmental BCP but should also familiarize themselves with the Branch plan and share it with their teams, include the staff in the testing and provide training where necessary, so that all affected staff members are aware of their roles and responsibilities in an incident.

If there is a change to staff, procedures or systems it is the responsibility of the Head of Department to inform the Chief Risk officer ("CRO") of these changes and it will be the responsibility of the Operational Risk Department to ensure the plan is updated to reflect these changes.

This departmental BCP's (see section 7) and Branch BCP should be reviewed at least annually and re-submitted to the ARCo for challenge and approval.

A copy of this plan will be readily available to the members of the IMT and the Heads of Department; it is therefore recommended that they keep copies of this plan in several places, for example, at the office, in a briefcase and at home. The plan contains sensitive data and should be stored securely at all times.

Heads of Department should also appoint a deputy for business continuity purposes, who should be fully briefed on this plan and as a minimum keep with them the relevant contact lists for their department.

The IMT will maintain an auditable log of actions taken for use during, and review after resolution of, the emergency situation. Logs will be retained for a period of 5 years from the date of closure of the log. The CRO will be responsible for arranging the secure storage of the logs.

The action log template is to be completed to record all major actions taken, the rationale for the decision and the approval for the decision. A log entry should be completed for each action.

Paper copies of the template will be stored at the business recovery site. The following example will be a template to record IMT actions:

IMT Emergency Action Log								
Unique ID	Source	Date raised	Field	Description	Owner	Comments	Target Date	Date Closed
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								

CNCBLB places significant reliance on HO for its business. In accordance with the Service Level Agreement between CNCBLB and CNCB has a responsibility to provide support for Business continuity arrangements to safeguard against disruption to the normal business activities of the Branch.

It is also important that HO includes CNCBLB in Group business continuity testing covering systems and technology to ensure that the London Branch is fully supported.

6. Dealing with the Media

All staffs should be fully aware that they must **not** to make **any** statements to the media.

If the media do approach any staff, then the reply given should be "***No Comment***".

The staff member can offer to take the persons details and pass them on to the President (such as police or ambulance staff), who will call them back at the earliest opportunity. Otherwise all inquiries should be referred to the Head HR and Administration who will liaise with the President and arrange a response on behalf of the business.

Depending on the scale of the incident the President may decide to issue a statement from the China CITIC Bank, London Branch, as this may be seen as being more suitable and have a positive impact the reputation of the bank.

Dealing with Casualties, Injuries or Fatalities

Any casualties will be cared for by the trained first aiders and if necessary emergency services will be called, to assist with the treatment of staff.

The HR and Administration Department and the Head of Department will liaise with and provide support to the staff and their family members. Staff emergency contacts/next of kin details are maintained by the Head of HR and Administration.

If the Police Family Liaison Officers become involved with the incident, HR and Administration Department will take the lead and develop this relationship and in some disasters this could continue for some time after the business has been recovered.

7. Departmental BCP's

Detailed requirements for specific business processes are identified in departmental Business Continuity Plans ("BCP").

IT systems recovery requirements are extrapolated from these departmental plans and amalgamated into an overarching IT systems recovery plan, supported by detailed system recovery plans. Key systems are identified in the analysis of the departmental business impacts.

Departmental business recovery plans are owned by department heads. They are responsible for maintaining and reviewing the plans and overseeing their implementation upon invocation.

Operational Risk Department will maintain the BCP register and manage any requirements and changes as defined within these BCP's.

REFER APPENDIX 3 - TEMPLATE FOR THE DEPARTMENTAL BCP

8. Business Impact Analysis

Each department has conducted a detailed departmental business impact analysis, with each business process being assessed for the impact of not being able to perform it. Impacts are assessed for non-financial factors to ascertain the bank's maximum tolerance for disruption.

Impact assessment is graded into four categories, Low, Medium Low, Medium High and High.

Category	Financial Value	Recovery Priority
High	>$5m	Yes - Required
Medium High	$250k to $5m	Yes - Required
Medium Low	$10k to $250k	BE - Best Efforts
Low	<$10k	No - Not Required

The BIA is assessed across different timeframes, from 4 hours to + 1 months.

The aim in developing business continuity strategies is to ensure that all processes reaching impact ratings of Medium High and High have been considered, and recovery procedures developed. Impacts rated Medium Low will be recovered on a best efforts basis.

The critical action required in an event, within the first 24 hours from availability of the DR site, identified the following actions required by departments in this period.

	AREA	ACTIVITY	Procedures	SYSTEM
First 4 hours	IT	Network management	Verify and resume network	Cisco Network
		Desktop support	Restart virtual desktops	Citrix Virutual Desktop
		Email support	Configure outlook for users	Outlook
		Business application support	Support users to access	NSSO/Teller/FMMS/520/Payment
	HR	Access to premises	Evacuation Process	N/A
		Co-ordinate fire officers and first-aid providers	Evacuation Process	N/A
		Manage relationship with landlords and building manager	Evacuation Process	N/A
		Employee relations	Employee Handbook	N/A
		Health & Safety	Employee Handbook	N/A
	RISK	Incident Management team	Operational Risk Policy	No system
	COMPLIANCE	Payment releases	AML/KYC policy	SWIFT
DAY 1	IT	Infrastructure management	Monitor and adjust	Device management interfaces
		Change management	Adjust system and user settings	Device management / NSSO
		System recovery	Restore destroyed systems	Vmware VDP
	FM	Execution of trades	Delegated Authority Policy	Reuters/FMMS
	OPS	Cash management / account payments & receipts	Operations Department Procedures	PSMG/CSOB
		Nostro/Custodian account Reconcilations	Operations Department Procedures	PSMG
		Nostro/Custodian account Statements	Operations Department Procedures	PSMG
		Custodian account reports	Operations Department Procedures	CLEARSTREAM
		Loan administration	Operations Department Procedures	520/CSOB
		FM Trade processing - current transaction	Operations Department Procedures	FMMS/PSMG/CSOB
		FM Trade processing - new transaction	Operations Department Procedures	FMMS/PSMG/CSOB
		FX processing / release	Operations Department Procedures	FMMS/PSMG
		Trade confirmation process	Operations Department Procedures	PSMG
		Netting of FM trades	Operations Department Procedures	E-MAIL
	COMPLIANCE	Suspicious transactions	AML/KYC policy	SWIFT

REFER APPENDIX 4 – 2020 BIA ANALYSIS (CRITICAL PROCESSES).

As per the BIA for the first 4 hours indicates, IT department will ensure the availability of the network, desktops, e-mail, business applications and general infrastructure support is available, which includes access to the telephones and internet access.

Once these are available, the following systems will be prioritized:-

PRIORITY SYSTEMS
Network
Vmware / Citrix / Netapp
Email
NSSO/Teller/FMMS/520/Payment
Reuters/Bloomberg
ODS
Vermeg

9. Third Party service providers

The aim of the BCP is to have continuous, high quality and prompt service from all third parties and where possible to minimize the risk of non-availability of service.

Reliance on Group Support

The Branch places significant reliance on CNCB for its business. In accordance with the Service Level Agreement HO has a responsibility to provide operational and technology support to the Branch.

Alternative and standby supply: Where possible the branch will identify alternative sources of supply which can run concurrently or be accessed within a reasonable timeframe.

Contractual agreement: Where relevant the branch will require contract and service level agreement for key supplies.

Third party contact list: Recovery procedures place reliance on availability and action of a number of third parties. In addition, the branch will need to manage relationships and contact a number of parties including, key clients and counterparties, China, regulators, premises service providers and the disaster recovery provider.

Operational Risk department will maintain a full list of third party contacts accessible from outside of the bank's systems and premises. The Head of Departments must ensure they have all the contact details to conduct business off-site.

Third party selection process: This process will analyze each potential supplier for financial viability and business continuity practice, in line with the Outsourcing Policy.

10. Emergency Plan and Evacuation Procedures

The procedures to be followed in the case of any emergency, including those that require evacuation of the building, have been drawn up in conjunction with the Landlord.

The procedures are outlined in the London Office *Emergency Plan and Evacuation Procedures* available to all employees in the Human Recourses policy.

The following appendices provide a summary of the procedures and details of the DR site that are relevant to the BCP.

APPENDIX 5 – 99 GRESHAM STREET EMERGENCY EVACUATION PROCEDURES

APPENDIX 6 – DR SITE MAPS AND DIRECTIONS

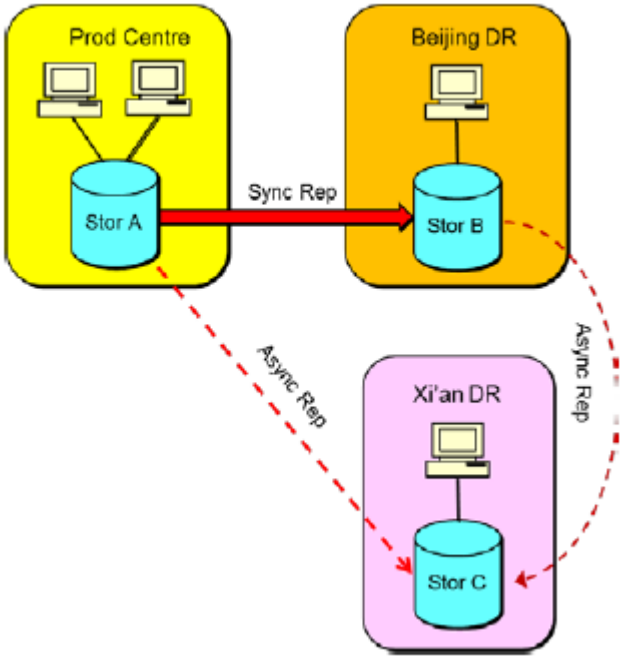
APPENDIX 1 – HO DR SYSTEM

HO has built a “Two Cities Three Centres” DR system. All three centres have the necessary network, server and storage deployed. The three centres have different objectives:

• The main production centre is located at Chaoyangmen, Beijing, where all production systems are installed;

• The “same-city” centre is located at Jiuxianqiao, Beijing, where some management systems and all same-city DR systems are deployed; and

• The remote centre is located in the city of Xi’an, to support the remote switchover of key systems in extreme conditions.



In the HO’s “Two cities three centres” DR system, the same-city DR is implemented at an application level, and will gradually evolve to ultimate provide “dual active” infrastructure. All significant systems can be switched over to same-city DR promptly, to meet the requirements of major accidental scenarios. The remote DR is used to help the Bank operate in extreme disasters. The core banking system and key channel systems can be switched over to the remote centre.

All other important systems duplicate data to the remote centre as well.

DR strategies and solutions are constituted according to the business characteristics of different business systems.

1) **Core banking system:** The core banking systems (including overseas core banking system) are running on IBM System i platform, and protected by MIMIX solution. Application data is copied from one production machine to 3 different standby machines (located in 3 centres). The core system can be switched to the same-city centre within one minute.

2) **Client-facing business systems:** Important business systems for external clients will deploy applications in both centres in Beijing running in a “dual active” mode. There will be no need to switch the applications if one site fails. The underlying databases are protected by disk replication or DB replication, which requires 10-20 minutes to switch over to DR. For example, the overseas teller system and international business system are protected by this kind of solution.

3) **Network**: The two data centres in Beijing are connected by raw fibre cable and DWDM to implement synchronous data replication and fast system switchover. The remote centre is connected by dedicated communication lines. A same-city network “dual active” solution is promoted to CNCB branches, to achieve the ability of instant network failover between a Branch’s two server rooms. The London Branch will also adopt this network DR solution locally.

The CNCB HO has established a comprehensive emergency management system, including contingency plans, DR drills, and emergency handlings.

- **Contingency plans:** Standard contingency plan templates are designed to cover all aspects, e.g. applications, network, storage, and IT infrastructure. And the contingency plans will be updated promptly after each system change, to keep their validity;
- **DR drills:** The HO will plan for DR drills in the beginning of each year. The drills include production system switchover, desktop drills and covers different scenarios like same-city failover, remote failover, accident recurrence and failure simulation. Each drill will involve business departments. The detailed process will be recorded, and all issues found will be retrospectively corrected; and
- **Emergency handlings:** Complete procedures are defined to deal with emergency situations. The emergency triggering conditions, and corresponding procedures including notification, organisation, reporting, decision, are all specified.

The IT systems used by CNCBLB are general production systems that will be shared by all CNCB overseas branches. Hence those systems are all installed in the Beijing production centre, with their backup systems in the same-city centre and remote centre.

All system changes will be submitted by CNCBLB (or other overseas branches) staffs to the HO Data Centre where the actual change operation will be executed.

In the event of DR drills, or system faults, the CNCBLB will cooperate with the Data Centre for the system emergency handling process.

APPENDIX 2 – CNCBLB DR SOLUTION

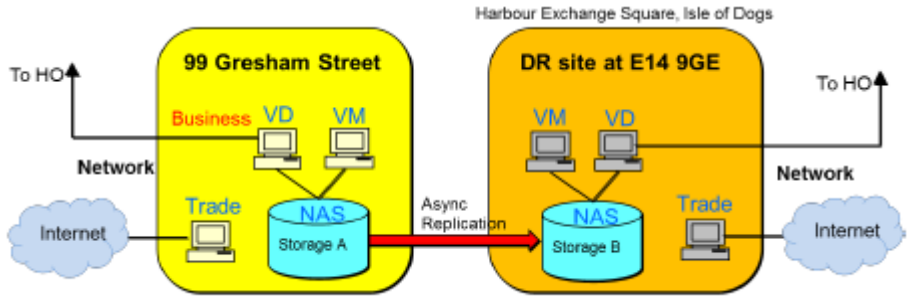
Although CNCBLB has no production systems physically installed in London, CNCBLB will deploy network infrastructure and some local supportive IT systems (e.g. virtual desktops and event monitors) to support the local daily business operations.

To ensure continuous business service, CNCBLB plans for necessary disaster recovery arrangements, including establishing a backup server room in London. In the backup server room, standby networking, server and storage devices would be installed. Important data of the Branch (primarily shared documents within the branch) is copied from the production server room to the backup server room. If the London production server room fails, the IT network and services will be restored in the backup server room and normal business services will resume.

In case of severe office damage, Branch IT staff will go to DR site for the manual DR fail-over of the following:

- Storage and Network Attached Storage ("NAS") (failover);
- Virtual machines and virtual desktops (import and restart); and
- Trade PCs (power on).

For the local DR solution above, the network can be switched over automatically. The planned RTO is set to be less than 2 hours, with the planned RPO approximately 2 hours using local data.



The Branch's contract will be with China Telecom, who will be the disaster recovery service provider. The CNCBLB DR site will be situated 4 miles away at:

01MC3A, 3rd floor, LD8, Harbour Exchange Square, Isle of Dogs, London, E14 9GE

The alternate office location has been chosen to be sufficiently far away from the main office such the likelihood of both sites being affected simultaneously is extremely remote.

Branch staff will have full access to the Bank's network and to all the business systems; London Branch will rent one rack from China Telecom at the DR site with simple furniture available.

APPENDIX 3 - Template for the Departmental BCP

Example – Risk Departments BCP

DEPARTMENTAL BUSINESS CONTINUITY PLAN

RISK

DATE 2020

HEAD OF DEPARTMENT Grant Lowe Approved

CRITICAL PROCESSES			BUSINESS RECOVERY REQUIREMENTS			
Process	Procedures	System	4 Hours	Day 1	2 to 7 days	> 7 days
1 Credit assessment	Credit Risk Policy	520	No	BE	Yes	
2 Credit Approval/Allocation	Credit Risk Policy	520 / FMMS	No	BE	Yes	
3 Credit monitoring	Credit Risk Policy	520 / FMMS	No	BE	Yes	
4 Market risk monitoring	Market Risk Policy	FMMS	No	BE	Yes	
5 Liquidity risk monitoring	Liquidity Risk Policy	No system	No	BE	Yes	
6 Operational risk event reporting	Operational Risk Policy	No system	No	No	No	Yes
7 Operational risk analysis/solutions/prevention	Operational Risk Policy	No system	No	No	No	Yes
8 Incident Management team	Operational Risk Policy	No system	Yes			
9 Key Risk Indicators	Operational Risk Policy	No system	No	No	No	Yes
10 Risk Profile /Risk Appetite reporting	Risk Appetite Statement	No system	No	No	Yes	

RESOURCES REQUIREMENTS (DR SITE)					
PRIORITY SYSTEMS	PEOPLE	4 Hours	Day 1	2 to 7 days	> 7 days
1 E-mail/ Network/internet	Grant Lowe	No	Yes		
2 520	Di Wu	No	No	No	Yes
3 FMMS	Xin Zhang	No	No	No	Yes
	Lily Bond	No	No	No	Yes
	Qiaoqiao Ren	No	No	Yes	

STAFF CONTACTS			
Maggie Boyce	Head of HR	xxxxxxxxxxxx	
Jinlei Xu	President	xxxxxxxxxxxx	
Gang Zhao	Vice-President	xxxxxxxxxxxx	
Grant Lowe	Chief Risk Officer	xxxxxxxxxxxx	
Rhod Sutton	Chief Compliance Officer	xxxxxxxxxxxx	
Colin Marshall	Head of Finance	xxxxxxxxxxxx	
HO CONTACTS			
Ms Li Shuxia	GM - Credit Approval	xxxxxxxxxxxx	lishuxia@citicbank.com
Mr Hu Kun	Head of Operational Risk	xxxxxxxxxxxx	hukun1@citicbank.com
Mr Sheng Biao	GM - Risk Management	xxxxxxxxxxxx	shengbiao@citicbank.com
THIRD-PARTY CONTACTS			
Aida Doddington	Bank of England (PRA)	xxxxxxxxxxxx	Aida.Doddington@bankofengland.co.uk
Dominic Chuah	Internal Auditors (BDO)	xxxxxxxxxxxx	dominic.chuah@bdo.co.uk

APPENDIX 4 – BUSINESS IMPACT ANALYSIS

2020 BUSINESS IMPACT ANALYSIS

	AREA	ACTIVITY	Procedures	SYSTEM
First 4 hours	IT	Network management	Verify and resume network	Cisco Network
		Desktop support	Restart virtual desktops	Citrix Virutual Desktop
		Email support	Configure outlook for users	Outlook
		Business application support	Support users to access	NSSO/Teller/FMMS/520/Payment
	HR	Access to premises	Evacuation Process	N/A
		Co-ordinate fire officers and first-aid providers	Evacuation Process	N/A
		Manage relationship with landlords and building management	Evacuation Process	N/A
		Employee relations	Employee Handbook	N/A
		Health & Safety	Employee Handbook	N/A
	RISK	Incident Management team	Operational Risk Policy	No system
	COMPLIANCE	Payment releases	AML/KYC policy	SWIFT
DAY 1	IT	Infrastructure management	Monitor and adjust	Device management interfaces
		Change management	Adjust system and user settings	Device management / NSSO
		System recovery	Restore destroyed systems	Vmware VDP
	FM	Execution of trades	Delegated Authority Policy	Reuters/FMMS
	OPS	Cash management / account payments & receipts	Operations Department Procedures	PSMG/CSOB
		Nostro/Custodian account Reconcilations	Operations Department Procedures	PSMG
		Nostro/Custodian account Statements	Operations Department Procedures	PSMG
		Custodian account reports	Operations Department Procedures	CLEARSTREAM
		Loan administration	Operations Department Procedures	520/CSOB
		FM Trade processing - current transaction	Operations Department Procedures	FMMS/PSMG/CSOB
		FM Trade processing - new transaction	Operations Department Procedures	FMMS/PSMG/CSOB
		FX processing / release	Operations Department Procedures	FMMS/PSMG
		Trade confirmation process	Operations Department Procedures	PSMG
		Netting of FM trades	Operations Department Procedures	E-MAIL
	COMPLIANCE	Suspicious transactions	AML/KYC policy	SWIFT
Day 2 To 7	IT	Data management / Backup	Backup new data at DR	Vmware / Netapp
		New device and infrastructure plan	Plan for DR growth and change	N/A
	HR&ADMIN	Payroll administration	Employee Handbook	N/A
		Recruitment, joiners/temp staff	Employee Handbook	N/A
		Manage salvage operation / recovery process / insurance	Evacuation Process	N/A
	BD	Business process	Credit Risk Policy	520/CRM
		Relationship management	Credit Risk Policy	N/A
		Products	New Product Policy	N/A
		Client on-boarding	Credit Risk Policy	520/CRM
		Target market	Market Risk Policy	N/A

		Loan pricing	Market Risk Policy	N/A
		Loan/interest repayment	Credit Risk Policy	N/A
		Loan details amendment	Credit Risk Policy	520
		Client communications		E-mail
	FM	Market Risk	Market Risk Policy	Reuters/Bloomberg
		Liquidity Risk	Liquidity Risk Policy	No system
		Credit Limit		FMMS
		Communications		Reuters/Bloomberg/Email
		Notifications		EMAIL
	OPS	Client notification / Agent Notification	Operations Department Procedures	E-MAIL / Fax
		Static data maintenance	Operations Department Procedures	FMMS/PSMG/CSOB
		New Accounts	Operations Department Procedures	CSOB
	FINANCE	Daily reconciliation		ODS
		Accounting entry		FMMS
		Balance sheet		ODS
		Income statement		ODS
		Liquidity risk monitoring		No system
		Regulatory reports		No system
	RISK	Credit assessment	Credit Risk Policy	520
		Credit Approval/Allocation	Credit Risk Policy	520 / FMMS
		Credit monitoring	Credit Risk Policy	520 / FMMS
		Market risk monitoring	Market Risk Policy	FMMS
		Liquidity risk monitoring	Liquidity Risk Policy	No system
		Risk Profile /Risk Appetite reporting	Risk Appetite Statement	No system
	COMPLIANCE	Client on-boarding		LN
		AML Management		LN
	CORP OFFICE	Branch Business Plan		No system
		Committee meeting minutes		OnBoard
Day > 7	IT	Remote DR access	Implement remote access for DR	Network
	HR&ADMIN	Building maintenance	Savils	N/A
		Pension administration	Employee Handbook	N/A
		Employee benefits	Employee Handbook	N/A
		Employee references	Employee Handbook	N/A
		Staff Appraisal process	Employee Handbook	BreatheHR
		Test evacuation process, liaise with emergency services	Evacuation Process	N/A
		Ensure fire officers and first-aid providers have training	Employee Handbook	N/A
	BD	Collateral Management	Credit Risk Policy	Collateral Management systems
	FM	New Products	New Product Approval Policy	FMMS
		Counterparty and Client on-boarding		CRM
	FINANCE	Account payable		SAP
		VAT		No system
		Corporate tax		No system
		HO reports		No system
	RISK	Operational risk event reporting	Operational Risk Policy	No system

		Operational risk analysis/solutions/prevention	Operational Risk Policy	No system
		Key Risk Indicators	Operational Risk Policy	No system
	COMPLIANCE	Sensitive information		EMAIL
		Regulations		EMAIL
	CORP OFFICE	Corporate Governance		No system
		Value & Mission statements		No system
		Branch policies & procedures		No system
		Corporate Office procedures		No system
		Delegation of Authority		No system
		Company House Information		Internet
		Internal Audit Function		Email
		UK Regulatory & HO Reporting		Internet

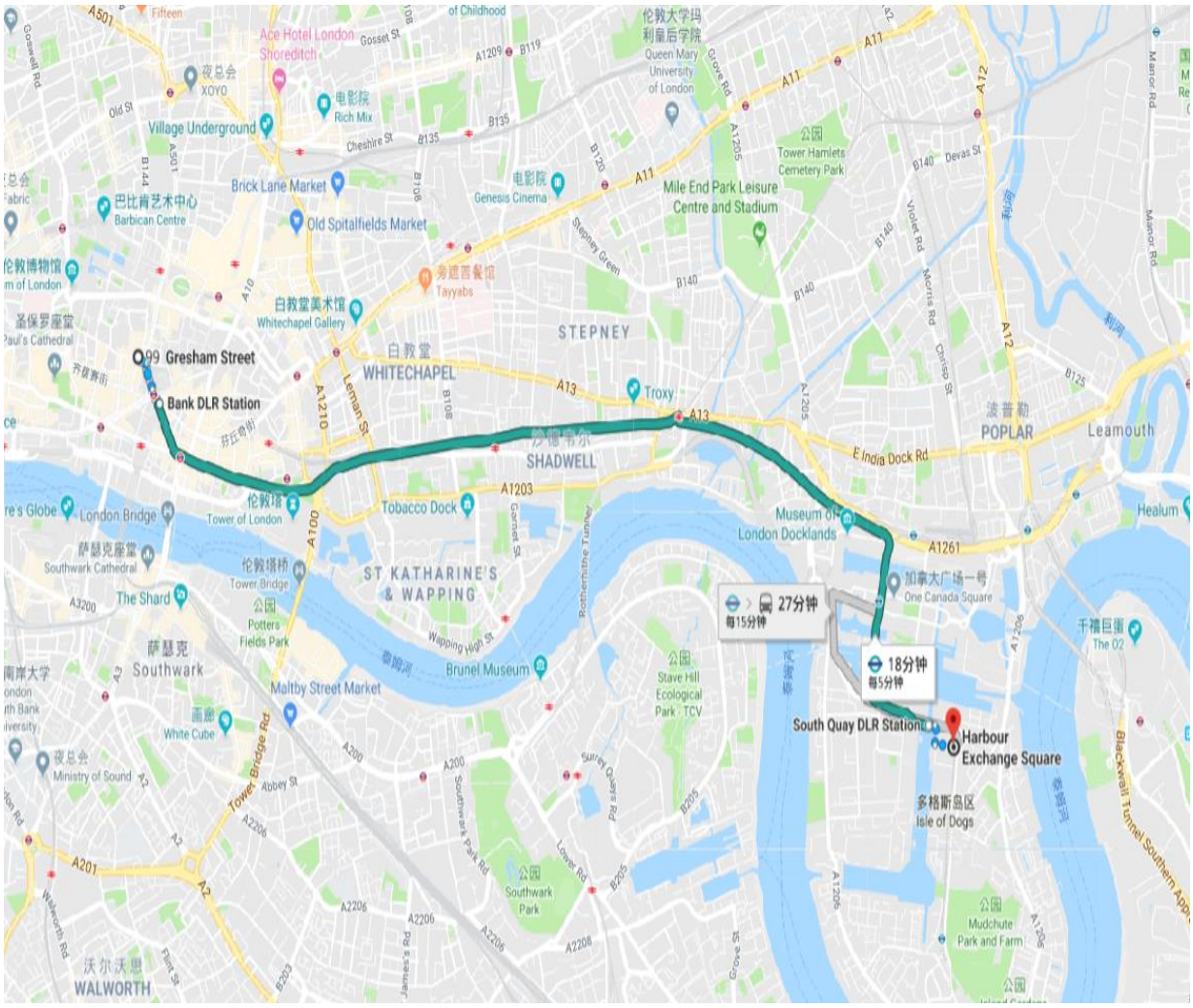
APPENDIX 5 - 99 GRESHAM STREET EVP

N:\PublicShare\HR\04 - Health and Safety\H&S Procedures

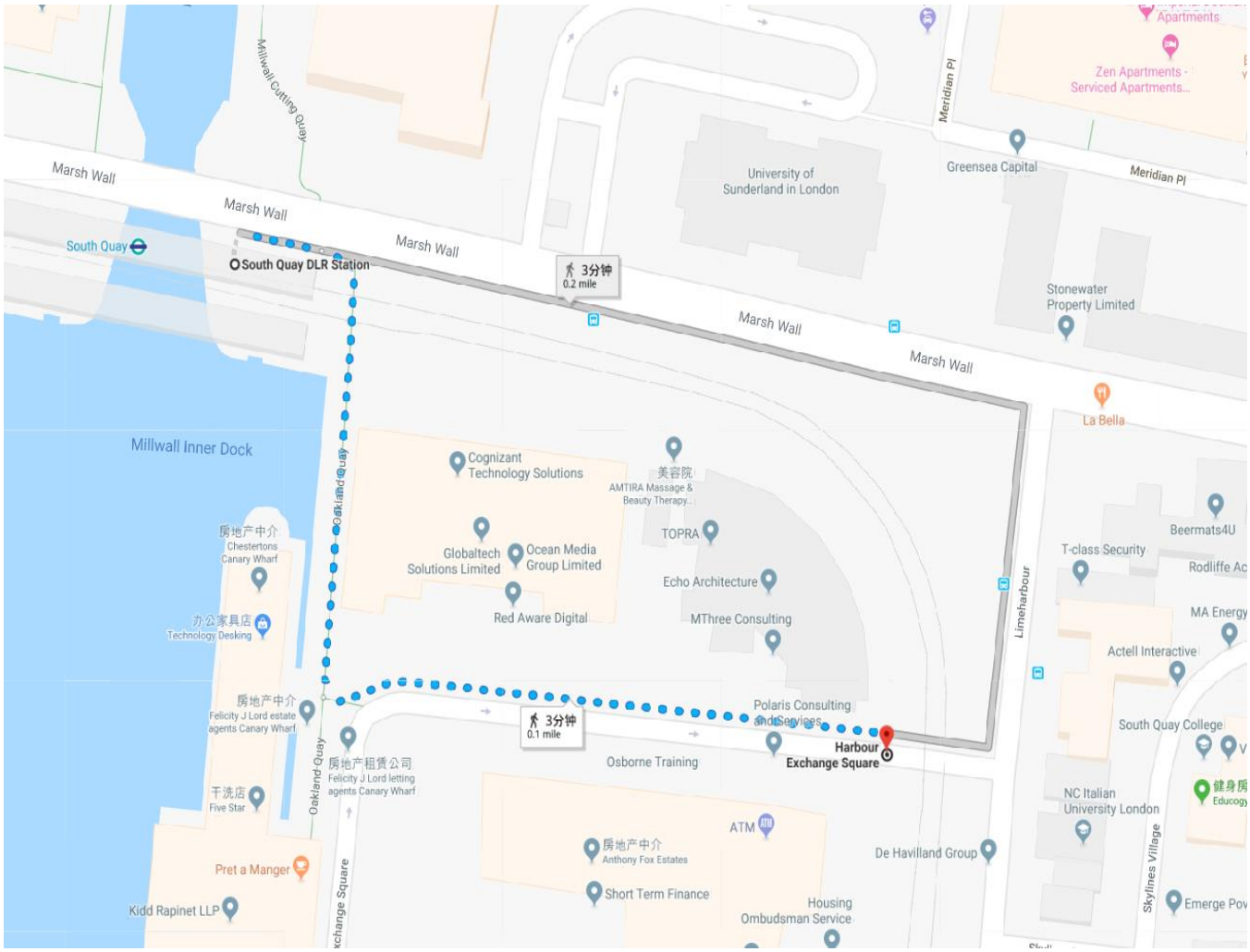
The above link is for the HR policy and procedures covering EVP, which is the Emergency Evacuation Procedures.

APPENDIX 6 – DR MAP & DIRECTION

CNCBLB subscribes a recovery rack of 01MC3A (No 65) at 3rd floor, LD8, Harbour Exchange Square, Isle of Dogs, London, E14 9GE. The map below shows the location of 3rd floor, LD8, Harbour Exchange Square, Isle of Dogs, London, E14 9GE.



Travelling: DLR from Bank Station to South Quay DLR Station


Millwall Cutting Quay
Marsh Wall
Marsh Wall
Marsh Wall
Marsh Wall
Marsh Wall
South Quay
South Quay DLR Station
3分钟
0.2 mile
Meridian Pl
Meridian Pl
University of Sunderland in London
Greensea Capital
Zen Apartments - Serviced Apartments...
Stonewater Property Limited
La Bella
Millwall Inner Dock
Oakland Quay
Cognizant Technology Solutions
美容院
AMTIRA Massage & Beauty Therapy...
TOPRA
Globaltech Solutions Limited
Ocean Media Group Limited
Red Aware Digital
Echo Architecture
MThree Consulting
房地产中介
Chestertons Canary Wharf
办公家具店
Technology Desking
房地产中介
Felicity J Lord estate agents Canary Wharf
3分钟
0.1 mile
Polaris Consulting and Services
Harbour Exchange Square
Osborne Training
房地产租赁公司
Felicity J Lord letting agents Canary Wharf
干洗店
Five Star
Pret a Manger
Kidd Rapinet LLP
ATM
房地产中介
Anthony Fox Estates
Short Term Finance
Housing Ombudsman Service
De Havilland Group
Limeharbour
Beermats4U
T-class Security
Rodliffe Ac
MA Energy
Actell Interactive
South Quay College
NC Italian University London
Skylines Village
Emerge Pov

APPENDIX 7 – POSSIBLE SCENARIOS

1. Denial of access to building

Physical access to 5F, 99 Gresham Street, London (EC2V 7NG) (primary site) could be denied for any number of reasons including:-

- Police cordon
- Fire
- Flooding
- Bomb alerts
- Gas leak or explosion
- Other natural or man-made events

If primary site is physically inaccessible then the following procedures should be implemented:

Source / IMT action
Whoever discovers the problem, should contact either their Head of Department or Head of HR or the President
This must be reported to IMT, who will advise strategy / actions required to all Heads of Departments
Actions for Head of Department
Contact all staff and advise them to convene at Fire Assembly Point.
Contact and confirm that all staff have been accounted for and advised of the situation.
Heads of Department to advise any visitors due at primary site that the building is currently inaccessible and meetings will have to be re-scheduled or conducted via audio.

Head of HR will direct the individuals or if more serious contact the President / IMT to invoke BCP

2. Power failure

Primary site has a UPS generator that will continue to provide power in the event that the main power supply is disrupted. Additionally, most providers of electric power use best endeavours to ensure that any disruption to the external supply is repaired within four hours.

However, if primary site is accessible but the power to the building is disrupted and likely to be out for some time then the following procedure should be implemented:

Source / IMT action
Whoever discovers the problem, should contact either their Head of Department or Head of IT or the President
This must be reported to IMT, who will advise strategy / actions required to all Heads of Departments
Actions for Head of Department
Contact and confirm that all staff have been accounted for and advised of the situation.
Identify the areas in your department affected by the power failure, also identify any spare capacity in your department that is not affected by the power failure.
Confirm whether the telephones are still working.

Head of IT will direct the individual or if more serious contact the President / IMT to invoke BCP

3. Systems failure

If primary site is accessible and the power to the building is unaffected but the Bank's system connectivity is disrupted then the following procedure should be implemented:

Actions for Head of Department
Contact Head of IT and apprise them of the situation, if possible confirm which systems are unavailable and which are working, if any.
Confirm whether the telephones and faxes are still working.

Head of IT will direct the individual or if more serious contact the President / IMT to invoke BCP

4. Travel disruption/ Inclement Weather

If staff are unable to travel to work due to disruption in the transport infrastructure, bad weather or a health pandemic then the following procedures should be implemented:

Source / IMT action
Whoever discovers the problem, should contact either their Head of Department or Head of HR or the President
This must be reported to IMT, who will advise strategy / actions required to all Heads of Departments
Actions for Head of Department
Contact staff to determine if there are alternative routes to work.
Contact HR and Administration Department and confirm that all staffs have been accounted for and advised of the situation. Also advise how many staffs are expected in to work and the potential impact on day to day processing.

5. Health Pandemic

If staff are unable to travel to work due to disruption from a health pandemic then the following procedures should be implemented:

Source / IMT action
The Head of HR and the President can invoke the BCP
The IMT will advise strategy / actions required to all Heads of Departments
Actions for Head of Department
Contact staff and advise of agreed strategy/action
Determine how many staffs are fit to work.
Contact HR and Administration Department and confirm staff have been accounted for and advised the situation. Also advise how many staffs are expected to work and the potential impact on day to day processing.

The IMT will appoint tasks to individual members to monitor and report, for example:

- Corporate office manager, arrange IMT meetings to determine strategy and monitoring frequency
- Head of HR, contact peers banks to find out actions taken
- Head of Administration, contact building management to determine safety of office
- CRO, conduct risk assessment